

2/pkts

1

A METHOD OF TRANSMITTING MINI-MESSAGES, AND A DEVICE
ASSOCIATED WITH THE METHOD

The present invention relates to a method of transmitting mini-messages. It also relates to a transceiver device associated with the method. The invention is applicable to the field of transmitting data through a transmission network. It is applicable more particularly to the field of transmissions in which the data transmission network is a mobile telephone network or an Integrated Services Digital Network (ISDN). An object of the invention is to transmit mini-messages through the transmission network between a caller and a called party at lower cost. However, a preferred application of the invention relates to transmitting a smart card code (such as a personal identification number (PIN)) to an authentication center by using a mobile telephone network as the transmission network.

Currently, it is known that a message can be transmitted from a caller to a called party through a transmission network, such a message being a data structure comprising from a few bytes or even a few tens of bytes (the message may then be referred to as a "mini-message") to several thousands of bytes. In the state of the art, to transmit a message, it is necessary to set up a call between a caller and a called party, to transmit the message through the link, and finally to clear down the call once the interchange between the caller and the called party is finished.

When transmitting mini-messages, such a procedure poses problems. At the scale of a mini-message, the time required to set up a call, plus the call time, plus the time required to clear down the call gives a transmission time that is too burdensome.

In addition, when the mini-messages are smart card codes, for example, several tens of thousands of transactions can take place through the transmission network every day. Such a high number of transactions,

associated with the state-of-the-art procedure gives rise to a load on the network that is very considerable. That load on the transmission network is tending to become increasingly large as a result of the ever-increasing number of applications that implement smart cards and of the ever-increasing number of associated transactions. It should also be specified that the use of a call through a transmission network is not free of charge. The resulting cost of sending mini-messages is non-negligible in view of the number of transactions.

An object of the present invention is to remedy those problems by proposing a method of transmitting such mini-messages. The method of the invention makes it possible to reduce the transmission time to a value that is as low as possible by transmitting data during the signaling phase associated with setting up a call through a transmission network. In addition, the method of the invention makes it possible to reduce the cost of calling through the transmission network.

Furthermore, the invention proposes a transceiver device for implementing the method of the invention.

The invention thus provides a method of sending a user message through a transmission network, the method being characterized in that:

a request is activated to set up a call channel between a caller and a called party; and

to set up the call channel, a signaling stage is performed during which a signaling message containing at least one spare field is interchanged between the caller and the called party;

and in that:

before the interchange between the called party and the caller, the user message is placed in the spare field of the signaling message; and

the setting up of the call channel is terminated once the user message has been received by the called

party and/or a reply to the receiver message has been received by the caller.

The invention also provides a transceiver device for transmitting a user message to a called party and for receiving a reply to the user message from a called party, said device being characterized in that it includes a dedicated memory, the dedicated memory serving to store the user message and/or the reply to the user message, the user message and/or the reply being sent in a spare field of a signaling message during a signaling stage.

The invention will be better understood on reading the following description and on examining the accompanying drawings. They are given merely by way of indication and they in no way limit the invention. In the figures:

Figure 1 shows a simplified architecture for a mobile telephone making it possible to implement the method of the invention; and

Figure 2 shows an implementation of the method of the invention in the form of an algorithm.

Figure 1 shows a preferred application of the invention. It shows a simplified architecture for a mobile telephone 1 implementing the method of the invention and connected to a base station 2 of a mobile telephone network 3 via a radio link 4. Thus, the telephone 1 is used to send or to receive a user message through a transmission network such as the network 3, for example. In particular for providing these transmit and receive functions, the telephone 1 is provided with an antenna 5 connected to a transceiver device 6. The device 6 is controlled by a microprocessor 7 under the control of a program 8 in a program memory 9 via a data, control, and address bus 10.

In this preferred example, in addition to its usual mobile telephony function, the telephone 1 is used as a communications interface, or a modem, between a distant

party 13 and a reader 11 for reading a smart card 12. The reader 11 is preferably placed in the telephone 1, but it could also be merely connected thereto via a wire link. Thus, the distant party 13 is a center for authenticating the smart card 12. The center 13 is connected directly via a link 14 or indirectly via a fixed telephone network 15, for example, to a connection circuit 16 of the network 3. Thus, the telephone 1 sends to the center 13 a secret code of the card 12 and an identification number, the secret code and the identification number being placed in a spare field of the signaling message. The data unit made up of the secret code and of the identification number is referred to below as the "identifier".

In the invention, the user message is transmitted during a signaling stage associated with setting up a call between the telephone 1 and the center 13. For this purpose, use is made of a field left spare in the signaling messages interchanged between the telephone 1 and the device 13, as described in particular in GSM Standard 04.18. That Standard also defines a procedure for setting up a call in a mobile telephone network, in particular complying with the GSM Standard.

A "spare field" implies that a signaling message is of variable length. Naturally, when the spare field is not used, the portion corresponding to a given field is transmitted only if said field contains information. A signaling message is thus made up of various fields, each of which relates to a parameter, one of which specifies, in particular, a function associated with said message. The message may be a control message or a message for monitoring the various signaling stages required for setting up a call.

The secret code is produced from a keypad 17, e.g. of the telephone 1. More precisely, in this preferred embodiment of the invention, when the smart card 12 is inserted in the reader 11, and once a code has been

entered on the keypad 17, then the microprocessor 7 activates a request to set up a call channel between the telephone 1 and the device 13.

According to a first essential characteristic of the invention, the microprocessor 7 uses one of the spare fields of a signaling message, prior to transmission, to place the user message in it. In the invention, the control message that is transmitted and that contains the user message is a special message. The special message is a signaling message in which a value of a parameter makes it possible to indicate to the called party, when said called party receives it, that a message is to be found in the field that is normally spare. To achieve this, it is possible to use a predefined value which indicates that the call protocol is known to the caller and to the called party. As a result, when the called party receives a signaling message containing such a parameter, then said called party knows where the user message is to be found. However, it is quite possible to produce a new value in addition to the predefined values and that would achieve the same result. Thus, the center 13 in turn transmits a signaling message which contains a reply to the user message, e.g. whether, as a function of the identifier transmitted with the user message, the authentication of the card 12 is positive or negative.

According to a second essential characteristic of the invention, the microprocessor 7 causes the call set-up to terminate once the message 4 has been received by the called party and/or once a reply to the message 4 has been received by the caller. That is to say that, if the telephone 1 transmits a message 4 and does not await a reply from the center 13, then said center can terminate call set-up. If, however, a reply is awaited by the telephone 1 (since, in this example said telephone is the transmitter of the user message), then it is the telephone that must terminate call set-up. In this document, it is considered that a call is fully set up

when the called party accepts the call, i.e., more simply, when the called party answers. In the invention, the called party does not answer, but nevertheless receives the user message via the signaling messages. As
 5 a result, the cost of a call is zero since, generally, it is necessary to answer in order to initiate metering.

In a variant, the device 13 or the called party may be another mobile telephone 18, connected to a base station 19, for example, of the network 3. In which
 10 case, the telephone 1 and the telephone 18 may interchange mini-messages such as the user messages. In addition, the telephone 1 may be connected to a computer 20 thus using the telephone 1 as a modem. Similarly, the telephone 18 may be connected to a computer 21.

15 When a modem (the telephone 1 in this example) sets up a call channel, then it interchanges signaling messages with the called party, e.g. the telephone 18, and a signaling message is associated with a register, i.e. a memory zone. Thus, when the program 8 issues a
 20 command to transmit the user message, it associates it with a first signaling message, and when the telephone 1 receives a reply to the user message then said user message is associated with a second signaling message. This command is associated with a dedicated memory 22
 25 which serves as a register. As a result, when the telephone 1 receives a reply to the user message, then said reply is stored automatically in the memory 22, generally under the control of a management sub-program associated with the program 8. Operation is the same at
 30 the center 13 and at the telephone 18, i.e. when the center 13 or the telephone 18 receive the user message, then said user message is stored in a dedicated memory (not shown), such as the memory 22. For smart cards, the center 13 thus stores in a dedicated memory a value for
 35 the secret code and a value for a card number, and a value stored in the register 22 may correspond to positive or negative acknowledgment by the center 13,

depending on whether the code is accepted or refused, respectively.

In a preferred example, a user is authorized to access the memory 22 via specific commands. Thus, the user may place values to be transmitted therein and/or read received values therefrom. For this purpose, the user uses, in particular, the keypad 17 of the telephone 1 or the keyboard of the computer 20 if said computer is connected to the telephone 1. In an example, the specific commands are commands for controlling a modem. However, depending on needs, a user may produce new specific commands that are specific to said user and that may be referred to as "proprietary" commands.

In a preferred variant of the invention, the memory 22 is placed in the telephone 1. By using a dedicated memory such as the memory 22, it is possible for operation of the telephone 1 to be more flexible. The user knows that when such a signaling message is received, it is necessary merely to perform a read operation for reading from the associated dedicated memory, using the above-mentioned sub-program, in order to determine the value corresponding to the received message 4. The telephone 13 and the telephone 18 operate in the same way as regards the use of a dedicated memory.

In another variant, the memory 22 is placed in a modem (not shown) of the ISDN type. Such modems make it possible to connect a caller to a called party via an ISDN that is then used as a transmission network of the invention. In which case, taking the example of the computer 20, said computer is connected to the modems instead of being connected to the telephone 1. A signaling stage via an ISDN uses signaling messages which, as in the mobile telephone network 3, contain spare fields.

In a preferred example of the invention, the size of the user message is limited to 35 eight-bit bytes at

maximum. A spare field can receive only data whose binary length is shorter than 35 bytes.

The function of the memory 22 is to store the user message and/or the reply to the user message, the user message and/or the reply being to be sent by means of a spare field in a signaling message. Thus, in the preferred example, the memory 22 has a memory capacity which is no more than 35 bytes. In another variant, and to enable the user message to be transmitted securely via the network 3 and the spare field, it is enciphered with an enciphering key so as to make one third of it incomprehensible. When the addressee of the user message receives the user message, then said addressee uses an associated deciphering key to make the information carried by the user message comprehensible.

Figure 2 shows an implementation of the method of the invention in the form of an algorithm. Authenticating the PIN of a smart card such as the smart card 12 is given by way of example. The transceiver device used for this purpose is the telephone 1 of Figure 1 with the reader 11. Thus, in a step 23, the PIN associated with the smart card 12 is entered by means of the keypad 17. Naturally, prior to this, the telephone 1 is configured for special operation, i.e. it operates as a smart card reader. A value for the PIN is stored in the memory 22 pending transmission of it.

In a formatting step 24, the program 8, or more precisely a sub-program of said program 8 causes the microprocessor 7 to forward the value stored in the memory 22 to the transceiver device 8 and thus to prepare the user message for transmission. The user message contains the PIN (enciphered in a preferred example), and it is inserted in a spare field of a signaling message. In a step 25, the signaling message containing the message 4 is transmitted to the authentication center 13 in this example. In a step 26, the center 13 proceeds to perform the authentication after deciphering the PIN

which, in this example, is received as associated in particular with the identification number of the smart card 12. Once the authentication is finished, the center 13 transmits the reply associated with said

5 authentication to the telephone 1, in a step 27.

In step 28, the telephone thus receives a reply to the user message transmitted in step 25, and it stores the reply from the center 13 in the memory 22. A processing program associated with the operation of the
10 telephone 1 as a smart card reader retrieves contents of the memory 22 in a step 29. If the authentication message is positive at the end of a test step 30, then, in a step 31, the microprocessor 7 authorizes payment by informing a holder of the card 12 via an audible and/or
15 visible message. When the authentication is negative, the authorization of step 31 is refused to the holder of the smart card 12. Thus, the invention makes it possible to reduce the time required to access the center 13 and thus the time required for the reply, while also thereby
20 limiting the cost of calling through the network 3.

This description is based on an example concerning the authentication of a smart card PIN, but naturally, the method of the invention may be used to transmit any message of a few tens of bytes to a called party. Thus,
25 the field of the invention more generally concerns transmitting data through a transmission network of the GSM or ISDN type.